



125 Park Avenue, 7<sup>th</sup> Floor  
New York, NY 10017  
Telephone (212) 655-3500  
Facsimile (212) 655-3535  
www.meisterseelig.com

Henry E. Mazurek  
*Partner*  
Direct (212) 655-3594  
Fax (646) 539-3694  
*hem@msf-law.com*

October 29, 2018

**By ECF and Federal Express**

Hon. Allyne R. Ross  
United States District Court  
225 Cadman Plaza East  
Brooklyn, New York 11201

**Re: *United States v. Yehuda Belsky*, 18 Cr. 504 (ARR)**

Dear Judge Ross:

We are writing on behalf of defendant Yehuda Belsky in support of his application to modify his conditions of pretrial release. Mr. Belsky is charged in a three-count Indictment, alleging violations of: (1) mail fraud (18 U.S.C. § 1341); (2) failure to register as a Commodity Trading Advisor (7 U.S.C. §§ 6m(1) and 13(a)(5)); and (3) misappropriation of customer funds (7 U.S.C. § 13(a)(1)). These allegations arise out of claims that Mr. Belsky made misrepresentations in the solicitation and use of funds from putative “investors,” and instead used such funds “he received to margin, guarantee and secure the trades and contracts of one or more customers,” (Indict., ¶ 22), for his own personal use and profits. Also, the indictment alleges that Mr. Belsky traded in options contracts without being registered as required by federal regulations and the relevant regulator, the Commodity Futures Trading Commission (“CFTC”), and for intentionally misappropriating customer funds without being registered as a commodity trading advisor.

**Background and Procedural History**

Mr. Belsky was arrested and presented for arraignment on these charges on September 26, 2016. At the presentment, Pretrial Services initially recommended a condition of pretrial release to include no computer usage at all by Mr. Belsky while on bail. After conferring, the parties jointly agreed this condition was overbroad to conform to the statutory requirements of the Bail Reform Act, codified at 18 U.S.C. § 3142(c). Instead, the government proposed that the condition should include electronic monitoring by Pretrial Services of all of Mr. Belsky’s personal devices that have the capacity of connecting to the Internet. Pretrial Services would

Hon. Allyne Ross  
October 29, 2018  
Page 2 of 6

utilize certain proprietary computer monitoring software to enforce this condition. This condition was imposed by Magistrate Judge Steven Tiscione to secure Mr. Belsky's release. *See* Order Setting Conditions of Release and Appearance Bond, 18 Cr. 504 (ARR), ECF Doc. 8 (attached at Ex. A) ("No use of computers or internet access without monitoring software").

At the time this condition was initially imposed, little details were disclosed regarding the application of the computer monitoring software. Since that time, we have learned that the monitoring software is incredibly comprehensive. The software implemented by Pretrial Services is called "RemoteCOM." *See* <http://remote-com.com>. A cursory review of RemoteCOM's website indicates that it was created to track a user's written material, communications, websites visited, or "chat rooms" engaged by the user. Primarily, it was established to monitor sex offenders' conduct on the web. *See e.g.*, "RemoteCOM User Agreement," at Exhibit B. This monitoring software records the total computer or internet usage by the defendant by capturing the keystrokes he enters on the computing device and taking a virtual video of all the typed content, search content, and any programs or sites visited by the monitored device. *See e.g.*, *United States v. Lifshitz*, 369 F.3d 173, 191 n. 10 (2d Cir. 2014) (describing monitoring software called "keystroke" monitoring which records not just defendants' website history, but also which programs they use, memos they write, e-mails they send – "in short, every keystroke").

The RemoteCOM software employed by Pretrial Services records everything Mr. Belsky does on the monitored device, including but not limited to: websites visited, software programs accessed, all text and e-mail communications, and, in essence, records any personal thought Mr. Belsky reduces to writing on his computer devices – even if they are totally unrelated to the charged offense conduct. Some of the unrelated content that the government is authorized to access includes issues concerning his minor children or wife; medical illnesses or conditions; family private affairs; and even attorney-client communications. Nothing that Mr. Belsky records on his phone, computer, personal assistant, or even smart-TV would be kept private under this overbroad monitoring. In today's world, when almost every activity or correspondence includes a computing device, this condition is unconstitutionally overbroad -- even for a defendant on pretrial release.

For the following reasons, the RemoteCOM monitoring is impermissibly overbroad violating Mr. Belsky's First, Fourth and Fifth Amendment rights and the limiting principles and mandates of the Bail Reform Act. Therefore, this condition should be vacated.

Hon. Allyne Ross  
October 29, 2018  
Page 3 of 6

### Argument

#### **The Computer Monitoring Condition of Pretrial Release is Overbroad and Not Narrowly Tailored to Meet the Statutory Requirements of the Bail Reform Act and Violates Mr. Belsky's First, Fourth and Fifth Amendment Rights**

The Bail Reform Act of 1984, 18 U.S.C. § 3141 *et seq.*, authorizes federal courts to place restraints on a defendant's liberty while criminal charges are pending. All questions with respect to Mr. Belsky's release must be examined under this statutory rubric. Though all federal defendants are presumed innocent, courts are authorized to detain a defendant prior to trial if, after a hearing, a "judicial officer finds that no conditions or combination of conditions will reasonably assure the appearance of the person and the safety of any other person and the community." 18 U.S.C. § 3142(e). Where, as here, the defendant is released pending trial, the court has a duty to select the "*least restrictive* further condition, or combination of conditions, that . . . will reasonably assure the appearance of the person and the safety of any other person and the community." 18 U.S.C. § 3142(c)(1)(B) (emphasis added); *see also United States v. Salerno*, 481 U.S. 739, 750-51 (1987) (upholding the constitutionality of a bail system where pretrial defendants could be detained only if the need to detain them was demonstrated on an individualized basis").

In making an individualized bail determination, courts may consider many factors, including the nature and circumstances of the offense; the weight of the evidence; the history and characteristics of the defendant; and the nature and seriousness of the danger to any person or the community. 18 U.S.C. § 3142(g).

The limited question posed by this motion to modify Mr. Belsky's conditions of release is whether requiring him to provide access to the government, through the attachment of RemoteCOM computer monitoring software to his personal electronic devices, of all of the content of his writings on those devices and search histories and actions taken on the Internet – is the least restrictive condition necessary to reasonably assure the safety of any other person and the community. *Id.* § 3142(c)(1)(B).

The government cannot show that this exhaustive computer monitoring is the "least restrictive condition" to reasonably assure the safety of other persons from being defrauded by Mr. Belsky in the future. *See United States v. Lifshitz*, 369 F.3d at 189-93 (reviewing application of computer monitoring software as condition of probation, including balancing government's interest with defendant's remaining expectation of privacy and scope and efficacy of condition).

Presumably, the government and Pretrial Services view this monitoring condition as necessary to prevent Mr. Belsky from soliciting and receiving funds from others for the purpose of making investments for which he is not licensed, such as commodities, futures and options trading. The imposed condition of monitoring his entire computer usage, however, is **not** reasonably related to this objective, and certainly not the **least restrictive** condition to accomplish it.

First, any defrauding of investors can occur without Mr. Belsky's use of a personal computing device. The same conduct can be completed using other people's computers, or without

Hon. Allyne Ross  
October 29, 2018  
Page 4 of 6

computer usage at all, by, for example, phoning in investments on trading exchanges. In fact, the most critical aspect of the alleged offense conduct – purported misrepresentations to solicit investments – can, and often is, effectuated without the use of a computer at all. Thus, the recommended condition is not narrowly tailored, or the least restrictive condition, to address the real harm sought to be avoided here. It also has very limited efficacy. *See Lifshitz*, 369 F.3d at 192 (finding that “the efficacy of the monitoring condition is not pellucidly clear. It is well known that experienced computer users are quite resourceful in circumventing the software employed, and federal officials have even publicly remarked upon this fact.”). Indeed, even if a defendant were monitored under this condition, there are innumerable computer services venues (*e.g.*, Staples, Office Depot, UPS, Kinko’s, etc.), which could be visited to accomplish the same conduct sought to be prevented by the personal monitoring imposed here.

Second, the scope of the RemoteCOM monitoring is vastly overbroad. As stated above, it is a “keystroke” monitoring system that captures everything the defendant does on the device. In *Lifshitz*, the Second Circuit reviewed this same form of monitoring as a condition for a convicted probationer. In that case, the Second Circuit vacated the monitoring condition and remanded proceedings for further review by the district court, citing its concerns that the “scope of the monitoring may [ ] be overbroad, and it is not clear from the record as it stands whether or not monitoring is sufficiently effective to justify its implementation.” 369 F.3d at 193 and n. 11. The Second Circuit noted the difference between the use of “filtering” software, aimed only at certain content or websites, and “monitoring” software, which “investigat[es] all of a probationer’s computer-based activities, including those performed locally without connection to the Internet or any network – such as [defendant’s] word processing activities or the financial accounting for his . . . business.” *Id.* at 191. The *Lifshitz* Court was concerned that the latter “continuous” monitoring was more akin to an unauthorized general search in violation of the probationer’s Fourth Amendment rights and “might be more like searching his diary or inspecting his closets than it is like the highly targeted diagnosis accomplished by drug testing.” *Id.* at 191-92. *See e.g., United States v. Jenkins*, 854 F.3d 181, 195 (2d Cir. 2017) (reversing special condition of supervised release requiring the defendant “notify his prospective employer of the nature of his conviction and the fact that his conviction was facilitated by the use of a computer” if the employment involved a computer; holding that the relationship between the restriction and the offense was not a “reasonably direct relationship”); *United States v. Lombardi*, 7727 Fed. Appx. 18 (March 22, 2018) (reversing condition of supervised release authorizing Probation to monitor any computer accessible to defendant to ascertain his compliance with other supervised release conditions as not reasonably necessary to protect the public and as being excessively harsh or inexplicably punitive).

Here, Mr. Belsky’s liberty and Fourth Amendment interests are broader than those analyzed by the Second Circuit in *Lifshitz*. Mr. Belsky still enjoys the presumption of innocence and any condition imposed under the Bail Reform Act must be narrowly tailored and be the least restrictive condition necessary to reasonably assure the safety of others. 18 U.S.C. § 3142(c). The government has offered no evidence to show how the “keystroke” monitoring applied here is the least restrictive and necessary condition to protect persons who might do investment business with Mr. Belsky. Indeed, Mr. Belsky already is subject to the standard condition, which prohibits him from committing any Federal, State or local crime while on pretrial release. If he were found to

Hon. Allyne Ross  
October 29, 2018  
Page 5 of 6

commit any financial crime while on bail, he would be in violation of this condition and subject to immediate detention and forfeiture of his bond.

Another condition of Mr. Belsky's bond prevents him from contacting any of the persons identified by the government as having done investment business with him, as alleged in the Indictment. This condition is narrowly tailored to the purpose of protecting these individuals' future safety. Adding an unfocused computer monitoring condition as proposed and applied here is not the least restrictive condition to accomplish the perceived goal of safety of others. For example, the government did not seek to put a GPS-tracking device on Mr. Belsky to monitor his movement to assure the Court that he is not traveling to a place where his alleged victims are. It did not do so because this condition would be overly restrictive under the Bail Reform Act and would be an undue deprivation of Mr. Belsky's liberty. *See United States v. Peterson*, 248 F.3d 79, 83 (2d Cir. 2001) (*per curiam*) ("Although a defendant might use the telephone to commit fraud, this would not justify a condition of probation that includes an absolute bar on the use of telephones."). Likewise, here, imposing continuous monitoring of all of Mr. Belsky's conduct on a computer is similarly overbroad and not the least restrictive condition necessary to reasonably assure he commits no future financial crime. Indeed, if the Court were to accept the government's position that this condition satisfies the Bail Reform Act's specific limitation to the least restrictive conditions necessary, this monitoring program could be implemented under the same justification on any defendant charged with a financial crime.

Third, the Second Circuit has provided this Court with some direction on a less restrictive monitoring condition. In *Lifshitz*, the Court describes another monitoring possibility through the records of a computer user's Internet Service Provider ("ISP"). An ISP records a user's Internet website browsing history. *Lifshitz*, 369 F.3d at 191. This type of monitoring would identify any electronic trading platform sites visited by Mr. Belsky from his identified devices. As a condition of release, Mr. Belsky could authorize his ISP (*e.g.*, Verizon, AT&T, etc.) to release records of his website browsing history for purposes of monitoring whether he visited any prohibited trading platforms. This alternative to the government's monitoring program is clearly less restrictive and its availability proves that the current "keystroke" monitoring program violates the Bail Reform Act. 18 U.S.C. § 3142(c). *See United States v. Lee*, 972 F.Supp.2d 403 (E.D.N.Y. 2013) (vacating pretrial release condition of requiring defendant to waive confidentiality of disclosures made to therapist while on pretrial release as being impermissibly overbroad and not the least restrictive condition necessary to reasonably assure the safety of the community under Bail Reform Act).

### **Conclusion**

For the foregoing reasons, this Court should find that the imposed pretrial release condition applying "keystroke" monitoring of Mr. Belsky's computing devices violates the Bail Reform Act, by not applying the "least restrictive condition, or combination of conditions," to "reasonably assure" the "safety of any other person and the community." 18 U.S.C. § 3142(c). The current RemoteCOM software monitoring unduly restricts Mr. Belsky's right to speech under the First Amendment and is an overbroad deprivation of liberty and privacy interests under the Fourth and Fifth Amendments. For these reasons, this Court should vacate the condition and

Hon. Allyne Ross  
October 29, 2018  
Page 6 of 6

impose a less restrictive condition of restricting Mr. Belsky's access to certain specified electronic securities trading platforms, which could be provided by the government.

Respectfully yours,

A handwritten signature in black ink, appearing to read 'H. Mazurek', written in a cursive style.

Henry E. Mazurek  
Evan L. Lipton  
*Counsel for Defendant Yehuda Belsky*

cc: A.U.S.A. Sarah Wilson Rocha